

Notice of Allowability

Application No.

09/874,364

Examiner

Virgil Herring

Applicant(s)

SCHEIDT ET AL.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to the amendment filed 26 May 2006.
2. ☒ The allowed claim(s) is/are 3-34, 37-65, and 67-70.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

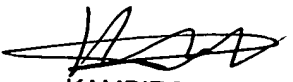
Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____
7. ☐ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____


KAMBIZ ZAND
PRIMARY EXAMINER

DETAILED ACTION

This action is responsive to the amendment filed 26 May 2006. Claims 3-34, 37-65, and 67-70 are currently pending. Of the above, claims 3-34 and 37-65 were previously allowed. Claims 1, 2, 35, 36 and 66 were previously cancelled.

Response to Amendment

Applicant's arguments, see page 14, filed 26 May 2006, with respect to claims 67-70 have been fully considered and are persuasive. The rejection of claims 67-70 under 35 USC §101 has been withdrawn.

Allowable Subject Matter

Claims 3-34, 37-65, and 67-70 are allowed.

The following is an examiner's statement of reasons for allowance:

Claims 3-34, 37-65, and 67-70 are drawn to a cryptographic key split combiner, a process for forming cryptographic keys, and storage media containing cryptographic keys produced by the process, respectively. The closest prior art, Hirsch (US Patent #5,276,738) in view of Albert et al (US Patent #5,627,894) discloses a similar key split combiner and process. Hirsch illustrates a cryptographic key split combiner and a process for combining comprising: a plurality of key split generators for generating cryptographic key splits (see column 1, lines 57-67); a key split randomizer for

randomizing the cryptographic key splits to produce a cryptographic key (see column 1, lines 54-57 and lines 62-68; column 2, lines 1-7; column 3, lines 60-65; and figure 1A, items 10, 12, and 16); in which each of the key split generators includes means for generating key splits from seed data (see column 1, lines 49-54 and lines 62-64); in which the plurality of key split generators includes a random split generator for generating a random key split based on reference data (see column 2, lines 55-58); and generating a pseudorandom sequence based on reference data (see column 2, lines 23-29). Albert et al specify generating a random sequence (see column 1, lines 51-67 and column 2, lines 1-2). However, they neither teach nor suggest generating a random sequence based on the reference data. This particular limitation incorporated into independent claims 3 and 37 renders claims 3-34, 37-65, and 67-70 allowable.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

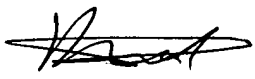
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Virgil Herring whose telephone number is (571) 272-8189. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Virgil Herring V H
Examiner
Art Unit 2132


KAMBIZ ZAND
PRIMARY EXAMINER

VH